

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE APPLICATION )  
OF THE UNITED STATES OF AMERICA )  
FOR AN ORDER AUTHORIZING THE ) Magistrate No. 19-mj-2608  
SEARCH OF 3 CELLULAR TELEPHONES, )  
AS LISTED IN ATTACHMENT A, SEIZED )  
INCIDENT TO ARREST )

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR SEARCH WARRANTS**

I, Melissa Laukaitis, Special Agent of the United States Drug Enforcement Administration (“DEA”), being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. This is an Affidavit provided in support of an application for a search warrant pursuant Federal Rule of Criminal Procedure 41. Specifically, I seek a search and seizure warrant authorizing the search and seizure of:

a. one (1) black Apple iPhone XS cellular telephone, bearing serial number F2LZ57GZKPHG and model number NT6J2LL/A and seized by law enforcement officers from the person of Quaruan CHANCE on December 30, 2019 (“**TARGET DEVICE 1**”);

b. one (1) silver and black iPhone 6 cellular telephone, bearing IMEI number 355402077873684 and model number A1586 and seized by law enforcement officers from the center console cup area of the vehicle Quaruan CHANCE was operating on December 30, 2019 (“**TARGET DEVICE 2**”); and

c. one (1) black iPhone cellular telephone, bearing FCC ID number BCG-E3085A and model number A1660 and seized by law enforcement officers from the center console

cup area of the vehicle Quaruan CHANCE was operating on December 30, 2019 (“**TARGET DEVICE 3**”) (collectively, the “**TARGET DEVICES**”).

2. The applied for warrant would authorize the forensic examination of the **TARGET DEVICES** for the purpose of identifying electronically stored data particularly described in Attachment B and using the protocols described in Attachment B by members of the DEA, or their authorized representatives, including but not limited to other law enforcement agents assisting the above described investigation. The **TARGET DEVICES** are currently in the custody of the DEA.

3. The **TARGET DEVICES** have been in secure law enforcement custody since the time they were recovered (the circumstances of which are explained more fully below). In my training and experience, I know that the devices have been stored in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the devices first came into the possession of law enforcement.

4. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516.

5. I am a Special Agent with the DEA, having been employed as such for approximately the past thirteen (14) years. I am currently assigned to the DEA Pittsburgh District Office, Group 62. As part of my duties, I am authorized to conduct investigations of persons who engage in drug trafficking offenses; specifically, the unlawful distribution of controlled dangerous substances in violation of Title 21 United States Code, Sections 841 and 846. I have obtained the information below through my direct involvement in this investigation and through other DEA Special Agents; Task Force Officers, State Officers, as well as reliable confidential sources.

6. Your Affiant has been involved in narcotics related arrests and the execution of search warrants which resulted in the seizure of narcotics, and assisted in the supervision of activities of informants who provided information and assistance resulting in drug buys. During the course of Your Affiant's training and experience, Your Affiant has become familiar with the methods and techniques associated with the distribution of narcotics, the laundering of drug proceeds, and the organization of drug conspiracies. In the course of conducting these investigations, Your Affiant has been involved in the use of the following investigative techniques: interviewing informants and cooperating witnesses, conducting physical surveillance, conducting and participating in short-term and long-term undercover operations including reverse undercover drug operations, consensual monitoring and recording of both telephonic and non-telephonic communications, analyzing pen register data, conducting court-authorized wire and oral interception electronic surveillance, and preparing and executing search warrants which have led to substantial seizures of narcotics, firearms, contraband, and evidence of criminal activity.

7. During my assignment with the DEA, I have participated in a wide variety of international and domestic investigations, including money laundering, drug trafficking, and airport interdiction. I have been the case agent for major narcotic investigations that led to the indictment of numerous individuals. I have been the affiant for, and participated in, numerous wiretap investigations during which I have monitored hundreds of hours of conversations between drug dealers.

8. I have received specialized training in multiple sessions and/or seminars on the sale and packaging of controlled substances, as well as firearms recognition and the characteristics of an armed gunman. I have utilized this training and experience and have participated in numerous significant arrests for illegal drug trafficking and/or the criminal possession/use of firearms. As a

result of these investigations, my training and experience, conversations with other agents, and interviews of drug users and traffickers, I am familiar with the methods and language used by traffickers to smuggle, store, and distribute drugs, collect and launder drug proceeds, and avoid getting caught by law enforcement officers.

9. As part of my duties, I am authorized to conduct investigations of persons who engage in drug trafficking offenses; specifically, the unlawful distribution of controlled dangerous substances in violation of Title 21 United States Code, Sections 841 and 846. I have obtained the information below through my direct involvement in this investigation and through other DEA Special Agents; Task Force Officers, and other local officers, as well as several reliable confidential sources.

10. Based on the facts set forth in this Affidavit, I submit there is probable cause to believe that Quaruan CHANCE ("CHANCE") has committed violations of Title 21 U.S.C. § 841, distribution and possession with the intent to distribute controlled dangerous substances. The statements contained in this Affidavit are based primarily on discussions with other law enforcement agents and witnesses, information provided to me by other law enforcement agents, review of documents and records, and my personal knowledge, observations, experience and training. Because this Affidavit is being submitted for the limited and specific purpose of supporting an application for search warrants for the **TARGET DEVICES**, I have not included every fact known to law enforcement concerning this investigation. I have not, however, omitted any facts that would tend to defeat a finding of probable cause.

**PROBABLE CAUSE**

11. On December 30, 2019, Pennsylvania State Police Troopers (the “Troopers”) observed a 2019 Jeep, bearing New York registration JFH7024 (the “2019 Jeep”),<sup>1</sup> traveling westbound on Interstate 76 near mile marker 80.7 in Westmoreland County, Pennsylvania and within the Western District of Pennsylvania. The Troopers observed the 2019 Jeep following too closely to another vehicle, changing lanes without signal, and driving in the left lane without a need to pass. Based upon these traffic violations, the Troopers initiated a traffic stop on the 2019 Jeep.

12. The Troopers identified CHANCE as the driver and sole occupant of the 2019 Jeep. Upon making initial contact with CHANCE, the Troopers observed him in possession of **TARGET DEVICE 1**. During the course of the traffic stop, the Troopers developed suspicion that CHANCE was involved in drug trafficking. Therefore, they asked CHANCE for consent to search the 2019 Jeep. CHANCE voluntarily consented to a search of the 2019 Jeep. The Troopers then began to search the 2019 Jeep. During the search, the Troopers located an aftermarket hidden compartment in the front center console of the 2019 Jeep.

13. After gaining access to the hidden compartment, the Troopers recovered approximately one kilogram of suspected cocaine from inside of the compartment. The approximately one kilogram of suspected cocaine was transferred to the DEA’s evidence control. Your Affiant field tested the suspected cocaine, which tested positive for cocaine, a schedule II controlled substance. I also weighed the cocaine, and the gross weight of the cocaine, including the heat-sealed packaging material, was 1.03 kilograms. Therefore, I believe that the total net

---

<sup>1</sup> The 2019 Jeep is registered to a female at an address in Island Park, New York.



weight of the cocaine, which does not include the weight of the heat-sealed packaging material, is at least 500 grams. I further believe that, based upon my training, knowledge, and experience, the possession of at least 500 grams of cocaine indicates an intent to distribute and not merely personal use.

14. The Troopers located a large quantity of United States Currency wrapped in rubber bands in the center console adjacent to the one kilogram of cocaine. Your Affiant knows, through my training, knowledge, and experience, that drug traffickers routinely possess large quantities of United States Currency as proceeds from their drug trafficking or as payment for additional quantities of drugs. The Troopers also recovered **TARGET DEVICE 2** and **TARGET DEVICE 3** in the center console cup area of the 2019 Jeep. Your Affiant knows, through my training, knowledge, and experience, that drug traffickers routinely utilize multiple cellular telephones to facilitate their drug trafficking for the purpose of eluding law enforcement detection.

15. Finally, from the 2019 Jeep, the Troopers also recovered a New York Police Department, Traffic Enforcement Division, Violation Tow Service, Vehicle Processing Record Receipt for a payment related to the 2019 Jeep dated December 10, 2019. CHANCE is listed as the individual from whom the payment was received.

**EVIDENCE COMMONLY GENERATED BY DRUG-TRAFFICKING AND  
ELECTRONICALLY STORED IN CELLULAR TELEPHONES**

16. Your Affiant is aware through both training as well as experience gained through multiple narcotics investigations, the targets of those narcotics investigations utilize cellular telephones to not only arrange meetings with their drug customers but also speak with fellow co-conspirators as well as their drug sources of supply. Your Affiant is also aware that these targets also utilize multiple cellular telephones at one time in an effort to not only thwart detection by law

enforcement but also to compartmentalize their drug trafficking customers to one phone, their co-conspirators to another phone, and their drug source of supply to yet another phone.

17. Based upon my training and experience, I am aware that it is generally a common practice for drug traffickers to store the names and phone numbers of drug customers and photographs and video detailing illegal activities in cellular telephones. Because drug traffickers in many instances will “front” (that is, sell on consignment) controlled substances to their clients, and/or will be “fronted” controlled substances from their suppliers, such record-keeping is necessary to keep track of amounts paid and owed, and such records will also be maintained close at hand so as to readily ascertain current balances. Often drug traffickers keep “pay and owe” records to show balances due for drugs sold in the past (“pay”) and for payments expected (“owe”) as to the trafficker’s supplier(s) and the trafficker’s dealer(s). Additionally, drug traffickers must maintain telephone and address listings of clients and suppliers and keep them immediately available in order to efficiently conduct their drug trafficking business.

18. Persons involved in significant drug trafficking typically conceal within automobiles large amounts of currency, financial instruments, precious metals, jewelry and other items of value, and/or proceeds of drug transactions and evidence of financial transactions relating to obtaining, transferring, secreting, or spending large sums of money derived from narcotic trafficking activities. This type of evidence can also be stored in applications that are commonly found on “SMART” cellular telephones, such as the **TARGET DEVICES** that are referenced throughout this affidavit.

19. Members of Drug Trafficking Organizations (“DTO”) often take group photographs with other enterprise members posing with paraphernalia, money and/or drugs. Many

cellular telephones have a camera feature that is readily capable of capturing and storing these group photos.

20. Members of DTOs often store each other's phone numbers and contact information in the directories of their cellular phones.

21. Based on my experience and familiarity with cellular telephones, I am aware that the telephones have voicemail and telephone directory features, as well as camera features which allow the user to take photographs and store them in the cellular phone's memory card. Based on my experience and training, statements by other law enforcement officers, and personal observations, I know that because of the storage capacity of cellular telephones, the portability of cellular telephones, the ease with which information stored on a cellular telephone may be accessed and/or organized, and the need for frequent communication in arranging narcotics transactions, cellular telephones are frequently used by individuals involved in drug trafficking. In particular, I and other law enforcement officers have found that information frequently maintained on cellular telephones includes the contact numbers of other co-conspirators, contact numbers for narcotics customers and stored photographs of DTO activities. This evidence will come in the form of caller identification information, call log information, telephone numbers, address information, or other identification information, as well as opened and unopened voicemail and/or text messages, photographs, videos and information about access to the Internet.

22. Members of DTOs routinely use multiple physical phones in succession as one breaks or the DTO feels that the number associated with the phone is compromised to Law Enforcement. The physical phone may no longer be an active communicative device, however many times, these old phones are not discarded as they possess value to the DTO. The replaced device contains within it the contact information for drug customers of the DTO, and many times



these phones are maintained as digital phone books should the new active phone become unusable or unavailable. Furthermore, these replaced phones are commonly kept in a relatively accessible location where either all or select members of the DTO can access the information within should it become necessary. As stated above, members of DTOs routinely take photographs and or memorialize other information of evidentiary value within these replaced phones. As such, it is common to recover a multitude of otherwise inactive phones especially at locations central to or important to the DTO.

### **TECHNICAL TERMS**

23. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communications through radio signals. These telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

24. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can

contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

25. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

27. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how each device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but

not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

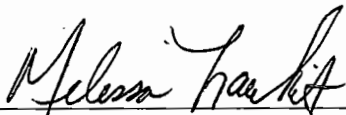
29. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

### **CONCLUSION**

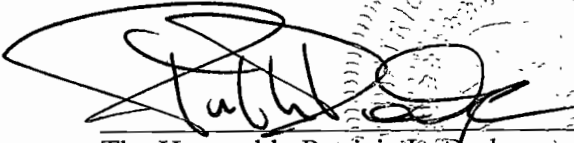
30. Based upon all of the foregoing, there is probable cause to conclude that, in the Western District of Pennsylvania, CHANCE violated Title 21 U.S.C. § 841, distribution and possession with the intent to distribute controlled dangerous substances. Further there is probable cause to believe that evidence of these crimes will be found upon searching the **TARGET DEVICES**.

31. WHEREFORE, I respectfully request that the Court issue a warrant authorizing members of the DEA, or their authorized representatives, including but not limited to other law enforcement agents assisting in the above described investigation, to search the **TARGET DEVICES**, as described in Attachment A, for the purpose of identifying electronically stored data particularly described in Attachment B and using the protocols described in Attachment B.

The above information is true and correct to the best of my knowledge, information and belief.

  
MELISSA LAUKAITIS  
Special Agent  
Drug Enforcement Administration

Sworn and subscribed to me this 31st day of December, 2019.

  
The Honorable Patricia L. Dodge  
United States Magistrate Judge



**ATTACHMENT A**

**Items to Be Searched**

The items to be searched are

- a. one (1) black Apple iPhone XS cellular telephone, bearing serial number F2LZ57GZKPHG and model number NT6J2LL/A and seized by law enforcement officers from the person of Quaruan CHANCE on December 30, 2019 (“**TARGET DEVICE 1**”);
- b. one (1) silver and black iPhone 6 cellular telephone, bearing IMEI number 355402077873684 and model number A1586 and seized by law enforcement officers the center console cup area of the vehicle Quaruan CHANCE was operating on December 30, 2019 (“**TARGET DEVICE 2**”); and
- c. one (1) black iPhone cellular telephone, bearing FCC ID number BCG-E3085A and model number A1660 and seized by law enforcement officers from the center console cup area of the vehicle Quaruan CHANCE was operating on December 30, 2019 (“**TARGET DEVICE 3**”) (collectively, the “**TARGET DEVICES**”).

The **TARGET DEVICES** are currently in DEA custody and are stored in a manner that is designed to preserve the electronic data. The **TARGET DEVICES** will be charged and powered on. The device(s) and all readable and searchable contents will be downloaded to a “CelleBrite” or “XRY” or similar device. The contents downloaded on the “CelleBrite” or “XRY” or similar device will then be copied to a readable computer disc and reviewed by your affiant. A search warrant return will be provided to the Court thereafter.

**ATTACHMENT B**

**Particular Items to be Seized**

Any and all fruits, contraband, records, evidence and instrumentalities relating to violations of Title 21, United States Code, Sections 841, including:

1. All records on the **TARGET DEVICES** described in Attachment A that relate to drug trafficking in violation of 21 U.S.C. § 841 including:

a. Evidence of communications referring to or relating to illegal narcotics or narcotics trafficking, including records of telephone calls, emails, instant messaging, or other records of communications, and including the identity of phone numbers, email accounts, or other electronic accounts used for such communications;

b. Evidence of communications with suppliers, purchasers, prospective suppliers, or prospective purchasers of illegal narcotics, including records of telephone calls, emails, instant messaging, or other records of communications, and including the identity of phone numbers, email accounts, or other electronic accounts used for such communications;

c. Evidence of communications referring to or relating to firearms and/or ammunition, including records of telephone calls, emails, instant messaging, or other records of communications, and including the identity of phone numbers, email accounts, or other electronic accounts used for such communications;

d. Documents, including photographs and video, depicting illegal narcotics, drug paraphernalia, firearms, ammunition, and violence related to the same;

e. Documents, including video and/or audio recordings, discussing and/or referring to illegal narcotics, drug paraphernalia, firearms, or ammunition;

f. Any and all information revealing the identity of co-conspirators in drug trafficking and/or firearm-related activity;

g. Any and all bank records, transactional records, records of wire transfers, checks, credit card bills, account information, and other financial records;

h. Any and all information suggesting sudden or unexplained wealth and/or unidentified conspirators;

i. Any and all information identifying the sources of supply and/or unidentified conspirators may have secured illegal narcotics, drug paraphernalia, firearms, and/or ammunition; and

j. Any and all information recording the scheduling of travel and/or unidentified conspirators, including destinations, dates of travel, and names used during travel.

2. All text messaging, call logs, emails, and/or other records of communication relating to the planning and operation of drug trafficking, in violation of 21 U.S.C. § 841.

3. Evidence of user attribution showing who used, owned, or controlled the **TARGET DEVICES** at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence.

4. Evidence of software that would allow others to control the **TARGET DEVICES**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

5. Evidence of the lack of such malicious software.

6. Evidence indicating how and when the **TARGET DEVICES** were accessed or used to determine the chronological context of **TARGET DEVICES** access, use, and events relating to the crimes under investigation and to the **TARGET DEVICES** user.

7. Evidence indicating the **TARGET DEVICES** user's state of mind as it relates to the crime under investigation.

8. Evidence of the attachment to the **TARGET DEVICES** of other storage devices or similar containers for electronic evidence.

9. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the **TARGET DEVICES**.

10. Evidence of the times the **TARGET DEVICES** were used.

11. Evidence of how the **TARGET DEVICES** were used and the purpose of its use including firewall logs, caches, browsing history, cookies, "bookmarked" or "favorite" web pages, temporary Internet directory or "cache," search terms that the user entered into any Internet search engine, records of user-typed web addresses, and other records of or information about the **TARGET DEVICES'** Internet activity.

12. Records of or information about Internet Protocol addresses used by the **TARGET DEVICES**.

13. Passwords, encryption keys, and other access devices that may be necessary to access the **TARGET DEVICES**.

14. Documentation and manuals that may be necessary to access the **TARGET DEVICES** or to conduct a forensic examination of the **TARGET DEVICES**.

15. Contextual information necessary to understand the evidence described in this attachment.

16. All serial numbers or International Mobile Equipment Identity (IMEI) numbers associated with any cellular telephones.

17. Log files, contact information, phone books, voicemails, text messages, draft messages, other stored communication, calendar entries, videos, and photographs related to matters described above.

In searching the **TARGET DEVICES**, the federal agents may examine all of the information contained in the **TARGET DEVICES** to view their precise contents and determine whether the **TARGET DEVICES** and/or information fall within the items to be seized as set forth above. In addition, they may search for and attempt to recover “deleted,” “hidden,” or encrypted information to determine whether the information falls within the list of items to be seized as set forth above.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any of the following:

- a. Any form of computer or electronic storage (such as hard disks or other media that can store data);
- b. Text messages or similar messages such as SMS or IM, saved messages, deleted messages, draft messages, call logs, all phone settings (*i.e.* call, messaging, display), priority senders, photographs, videos, links, account information, voicemails and all other voice recordings, contact and group lists, and favorites;
- c. Pictures, all files, cloud files and relevant data without password access, storage information, documents, videos, programs, calendar information, notes, memos, word documents, PowerPoint documents, Excel Spreadsheets, and date and time data;



d. Payment information, to include account numbers, names, addresses, methods of payment, amounts, additional contact information, and financial institutions;

e. Lists and telephone numbers (including the number of the phone itself), names, nicknames, indicia of ownership and/or use, and/or other contact and/or identifying data of customer, co-conspirators, and financial institutions;

f. Applications (Apps), to include subscriber information, provider information, login information, contact and group lists, favorites, history, deleted items, saved items, downloads, logs, photographs, videos, links, messaging or other communications, or other identifying information;

g. Social media sites to include, name and provider information of social media network(s), profile name(s), addresses, contact and group lists (*i.e.* friends, associates, etc.), photographs, videos, links, favorites, likes, biographical information (*i.e.* date of birth) displayed on individual page(s), telephone numbers, email addresses, notes, memos, word documents, downloads, status, translations, shared information, GPS, mapping, and other information providing location and geographical data, blogs, posts, updates, messages, or emails;

h. Any information related to co-conspirators (including names, addresses, telephone numbers, or any other identifying information);

i. Travel log records from GPS data (*i.e.* Google Maps and/or other Apps), recent history, favorites, saved locations and/or routes, settings, account information, calendar information, and dropped pinpoint information;

j. Internet service provider information, accounts, notifications, catalogs, Wi-Fi information, search history, bookmarks, favorites, recent tabs, deleted items and/or files, downloads, purchase history, photographs, videos, links, calendar information, settings, home

page information, shared history and/or information, printed history and/or information, or location data;

k. Email data, including email addresses, IP addresses, DNS provider information, telecommunication service provider information, subscriber information, email provider information, logs, drafts, downloads, inbox mail, sent mail, outbox mail, trash mail, junk mail, contact lists, group lists, attachments and links, and any additional information indicative of operating a sophisticated fraud scheme, or other criminal violations;

l. Any handmade form (such as writing);

m. Any mechanical form (such as printing or typing); and

n. Any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, cellular telephones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.